ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

Owner Information Privacy Protection Based on Internet of Vehicles

Hanbing Yu

School of Artificial Intelligence, Leshan Vocational and Technical College, Leshan, China

Abstract: *With the continuous development of Internet of Vehicles technology, more and more vehicles and drivers are joining the system. In this connected world, car owners' personal information is vulnerable to hacking and misuse. This paper analyzes the application status of Internet of Vehicles technology and the importance of vehicle owner information protection, Discuss the necessity and challenges of car owner information privacy protection. The study found that the protection of vehicle owner information needs to comprehensively consider technical, legal and management factors, by strengthening technical support, improving the legal system and strengthening management and supervision, protect the information security of car owners and promote the healthy development of Internet of Vehicles technology.*

Keywords: *Internet of Vehicles, Owner Information, Privacy Protection, Technology, Law, Management*

1. Introduction

Internet of Vehicles technology is a new type of technology based on intelligent transportation systems, which can realize information exchange and data sharing between vehicles, traffic facilities and drivers. The emergence of this technology has improved the safety, efficiency and convenience of road traffic, but it has also brought risks to the personal information of car owners [1]. With the continuous development of Internet of Vehicles technology, the protection of vehicle owners' information has become increasingly prominent. The purpose of this paper is to analyze the application status of Internet of Vehicles technology and the importance of vehicle owner information protection, discuss the necessity and challenges of vehicle owner information privacy protection, and put forward corresponding countermeasures [2].

2. Background

2.1 Overview and application scenarios of the Internet of Vehicles

The Internet of Vehicles refers to a technical system that connects vehicles, roads, and the Internet through wireless communication technology. It effectively integrates vehicles, roads, and the Internet， Intelligent interconnection between vehicles, between vehicles and road infrastructure, and between vehicles and the Internet is achieved. The application scenarios of the Internet of Vehicles are very wide, including but not limited to the following aspects:

Intelligent driving: Internet of Vehicles technology can realize autonomous driving, assisted driving and intelligent transportation systems, improving driving safety and efficiency. Through real-time communication and perception between vehicles, functions such as automatic vehicle following and fleet coordination can be realized [3]. Vehicle management and maintenance: The Internet of Vehicles can remotely monitor the status and performance of vehicles, Implement vehicle fault diagnosis. At the same time, it can also provide functions such as vehicle positioning and anti-theft tracking.

Intelligent traffic management: Through Internet of Vehicles technology, functions such as intelligent traffic signal control, traffic congestion warning, and intelligent navigation can be realized to improve traffic smoothness and reduce the incidence of traffic accidents [4]. Infotainment and services: The Internet of Vehicles can provide a wealth of infotainment and service functions, such as music and video playback, real-time weather forecasts, intelligent navigation, etc. It can also be interconnected with mobile devices to achieve remote control of vehicles and remote shopping.

Environmental protection and energy management: Internet of Vehicles technology can monitor and

ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

control vehicle energy consumption and emissions, optimize vehicle energy efficiency, and provide environmental pollution monitoring and reporting services.

2.2 The importance of vehicle owner information protection

Risk of personal information leakage: Internet of Vehicles technology can realize the sharing and transmission of vehicle location, driving trajectory, driving habits, vehicle condition information, etc. through communication between vehicles. However, this data contains a large amount of personal information. If not protected, it will be Facing risks such as information leakage and identity theft. Information abuse and commercial exploitation: Car owners' information contains a large amount of sensitive information, such as names, addresses, bank card numbers, etc. If this information is abused or commercialized, it will cause huge losses to car owners.

Legal and regulatory requirements: In some countries and regions, laws and regulations require automobile manufacturers and service providers to protect the privacy of car owners, otherwise they will face penalties, compensation and other related legal responsibilities. User experience and trust: For car owners, if their personal information is not properly protected, it will reduce their trust and experience in the Internet of Vehicles technology, and will also affect the development of the entire Internet of Vehicles industry.

Therefore, the protection of car owner information privacy is an inevitable trend in the development of Internet of Vehicles technology and an important factor in protecting the rights and interests of car owners and promoting the sustainable development of the Internet of Vehicles industry. Only through effective privacy protection measures can information sharing and utilization be achieved in the application of Internet of Vehicles technology.

3. Related work

3.1 Cutting-edge technologies and research results

At present, there are many cutting-edge technologies and research results in the field of Internet of Vehicles.

5G communication technology: 5G technology provides higher bandwidth and low latency, providing better support for real-time communication and large-scale connectivity of the Internet of Vehicles. With 5G networks, vehicles can quickly and reliably communicate with other vehicles, road infrastructure, and cloud servers.

Autonomous driving technology: Autonomous driving is an important direction of the Internet of Vehicles. Through lidar, cameras, sensors and other technologies, vehicle environment perception and autonomous decision-making are realized, and driving safety and efficiency are improved. Some companies have developed prototype vehicles with self-driving capabilities and tested them in specific road environments.

Edge computing and artificial intelligence: The Internet of Vehicles needs to process a large amount of data, including vehicle status, traffic information, etc. Edge computing and artificial intelligence technology can push data processing and decision-making to the vehicle itself or edge devices, reducing data transmission delays and network loads, and improving system response speed and stability.

Vehicle Cybersecurity: Security of connected cars is an important issue involving the protection of vehicles and data. Researchers are working to develop secure communication protocols, encryption algorithms and intrusion detection systems to protect vehicle networks from attacks and malicious manipulation. When the vehicle data in the system is tampered with or the vehicle is attacked, the malicious vehicle can be tracked through the combination of blockchain and big data.

Blockchain technology: Blockchain technology can provide a distributed, tamper-proof data storage and transaction mechanism. In the Internet of Vehicles, blockchain can be used for vehicle identity authentication, data sharing, and credibility verification of transactions, enhancing trust and security between vehicles.

The application of these cutting-edge technologies and research results will further promote the development of the Internet of Vehicles, improve the level of intelligence and interconnection of vehicles, and provide car owners with a safer and more efficient travel experience, as shown in Figure 1.

ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

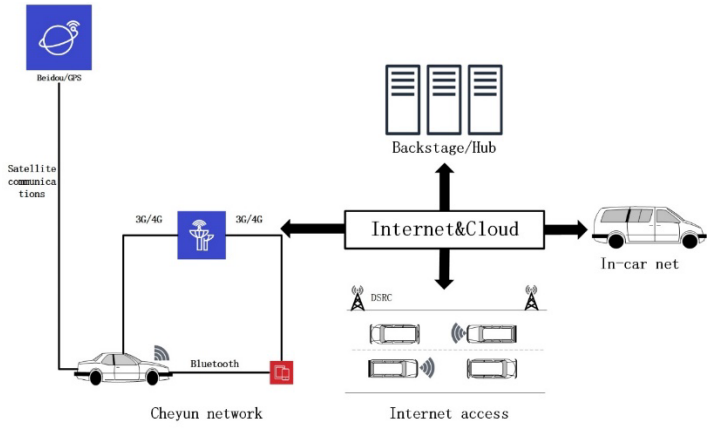

Figure 1: Internet of Vehicles System

3.2 Evaluation and analysis of existing privacy protection schemes

At present, there are a variety of privacy protection schemes in the field of Internet of Vehicles Data anonymization and desensitization: this is a common privacy protection method to protect the privacy of car owners by removing or replacing personally identifiable information in sensitive data, such as names, mobile phone numbers, etc. However, data anonymization and desensitization are not a completely reliable privacy protection scheme due to the risk of re-identification of personal information due to the relevance of data and the disclosure of background knowledge.

Encryption technology: Encryption technology can effectively protect the privacy of car owner information and ensure that the data is not read or tampered with by unauthorized visitors during transmission and storage. Existing encryption schemes include end-to-end encryption of communication data, the use of secure key management mechanisms, and more. However, encryption also faces performance and efficiency issues when processing large-scale data.

Access control and authority management: Through access control and authority management, the access and use of vehicle owner information is restricted, and only authorized users or systems can obtain relevant data. This method can effectively protect the privacy of car owners, but it is necessary to establish a sound access control strategy and permission management mechanism, and carry out effective monitoring and auditing.

Data ownership and sharing mechanisms: Car owners can protect their privacy with clear data ownership and sharing mechanisms. For example, car owners can selectively share their driving data and reach an agreement with the data user to clarify the purpose and scope of data use, and limit the misuse and commercial use of the data. This approach requires the establishment of a credible data exchange platform and a rights protection mechanism.

Privacy protection laws and regulations: Many countries and regions have formulated relevant privacy protection laws and regulations, requiring Internet of Vehicles service providers to comply with certain privacy protection regulations and bear corresponding legal responsibilities for privacy leakage. This approach protects the privacy rights and interests of car owners through legal means, but it still requires the establishment of an effective regulatory and enforcement mechanism. In summary, existing privacy protection solutions have their own advantages and disadvantages, and no one solution can completely solve all privacy protection problems.

Therefore, the comprehensive use of a variety of privacy protection technologies and methods, combined with the support and supervision of laws and regulations, can better protect the privacy rights and interests of car owners. At the same time, with the continuous development of technology and in-depth research, it is also necessary to continuously improve and update privacy protection solutions to meet new privacy and security challenges.

ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

4. The key technology of car owner information privacy protection

4.1 Data Encryption and Privacy Protection

Data encryption is a common privacy-preserving method that encrypts data so that it cannot be read or understood by unauthorized users.

Symmetric encryption: Symmetric encryption is a method of encryption and decryption using the same key. The data sender and receiver need to share a key. Beforehand, with the data sender using the key to encrypt the data and the receiver using the same key to decrypt the data. Symmetric encryption algorithms have high efficiency and fast encryption and decryption speeds, but there may be certain security challenges in key management and distribution, as shown in Figure 2.

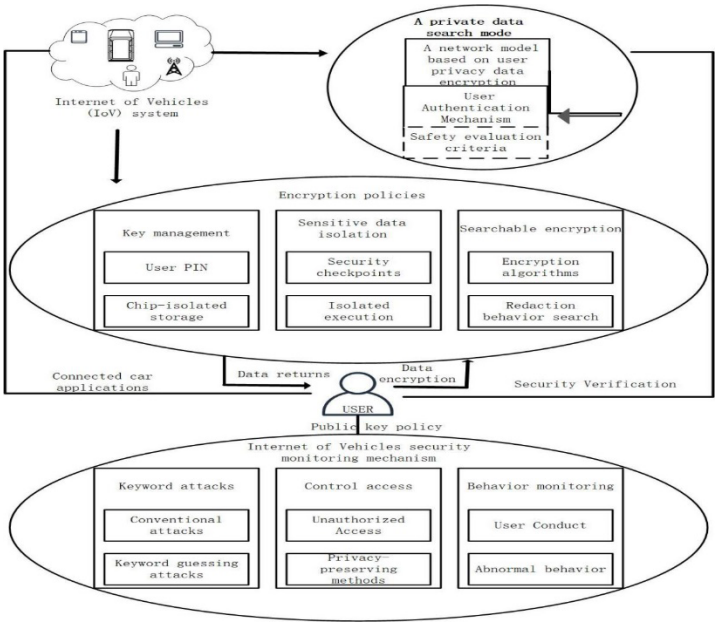

Figure 2: Internet of Vehicles Privacy Encryption

Asymmetric encryption: Asymmetric encryption uses the pairing of public and private keys for encryption and decryption. The sender encrypts the data with the receiver's public key, and the receiver can only decrypt the data if the receiver has a private key paired with its public key. The asymmetric encryption algorithm provides a better key management and distribution mechanism, and can implement functions such as digital signatures, but the encryption and decryption speed are slower.

Hybrid encryption: Hybrid encryption is a combination of symmetric and asymmetric encryption. During transmission, an asymmetric encryption algorithm is used to exchange the keys used for symmetric encryption, and then the data is encrypted for transmission using a symmetric encryption algorithm. In this way, the key management of asymmetric encryption and the efficiency of symmetric encryption can be taken into account.

End-to-end encryption: End-to-end encryption is a mechanism that protects the privacy of communication content by establishing an encrypted channel between the sender and receiver of the data, so that even during data transmission, intermediate nodes cannot read or tamper with the data. This encryption ensures the security of data in transit and at rest.

Data protection protocols and standards: In order to ensure the consistency and interoperability of data encryption and privacy protection, many organizations and standardization bodies have formulated relevant data protection protocols and standards, such as TLS/SSL protocol, IPsec protocol, etc. These protocols and standards provide a unified encryption and privacy protection mechanism to ensure the security of data transmission and storage.

4.2 Anonymization technology and identity authentication mechanism

Anonymization technology and identity authentication mechanisms are another common method of privacy protection designed to protect individual identities and sensitive information.

ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

Data anonymization: Data anonymization is the process of removing or replacing sensitive personally identifiable information so that data cannot be directly associated with a specific individual. Common anonymization techniques include desensitization, data generalization, and data masking. Anonymization can reduce the risk of personal identification of individuals, but it is important to note that anonymization does not guarantee that data will not be re-identified, so it needs to be combined with other technologies and measures to enhance privacy protection.

Authentication mechanism: The authentication mechanism is used to confirm the identity of a user and control their access to a system or service. Common authentication methods include username and password, fingerprint recognition, voiceprint recognition, face recognition, and two-factor authentication. Authentication mechanisms protect personal privacy and data security by ensuring that only authenticated users can access sensitive data or perform specific actions.

Anonymous Identity: Anonymous identity can be a solution for effective interactions and services while protecting the privacy of individuals. Anonymous identity is the anonymization of a user's identity, enabling users to interact and use services without revealing their true identity. This method reduces the risk of personal privacy leakage by isolating the user's real identity from the anonymous identity.

Blockchain technology: Blockchain technology can provide a decentralized identity authentication mechanism to ensure that users' identity information is mastered and managed by users. Through the distributed ledger and cryptography algorithms of the blockchain, secure, tamper-proof authentication can be achieved and users can provide better privacy protection.

Privacy protection laws and regulations: Many countries and regions have enacted relevant privacy protection laws and regulations that require the lawful, fair and secure processing of personally identifiable information. These laws and regulations stipulate the principles of personal information processing, the requirements for the protection of rights and interests, and the penalties for violations, etc., and provide a legal basis and regulatory support for privacy protection.

Design and implementation of privacy protection schemes.

Privacy risk assessment: First, conduct a comprehensive privacy risk assessment of the data processing environment and application scenarios. The assessment needs to identify the types of sensitive information that may be involved, potential privacy breaches during data collection, storage, and transmission, as well as the requirements of relevant laws, regulations, and privacy protection standards. Data classification and identification: Classify and identify data based on the results of privacy risk assessment. Divide your data into different levels of sensitivity and assign privacy protections to your specific needs, as shown in Figure 3.

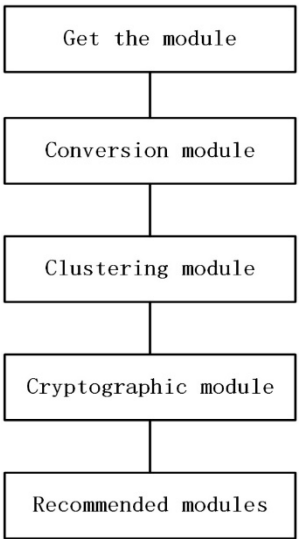

Figure 3: User privacy protection system

Anonymization and redaction techniques: Anonymization and redaction techniques may be used for data involving personally identifiable information. For example, removing or replacing sensitive fields, obfuscating, data generalization, etc., to reduce the identification of personally identifiable information. Encryption and access control: For sensitive data that needs to be protected, use encryption technology to ensure the security of the data during storage and transmission. At the same time, a strict access control

ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

mechanism is adopted to restrict access to sensitive data to only authenticated and authorized users.

Authentication and authorization: Establish an effective authentication and authorization mechanism to ensure that only authenticated users can access sensitive data or perform specific actions. Use methods such as multi-factor authentication, single sign-on, access tokens, and more to enhance the security of authentication. Data audit and monitoring: Implement a data audit and monitoring mechanism to monitor and record the use and access of data, so as to detect abnormal behaviors or privacy leakage incidents in a timely manner and take corresponding countermeasures. Education and training: Provide relevant privacy protection education and training for employees and users, enhance their awareness and understanding of privacy protection, and promote the establishment of compliance behaviors and privacy protection culture.

Privacy Policy and Compliance Management: Establish a clear privacy policy and ensure that it complies with applicable laws, regulations, and privacy protection standards. Establish a compliance management system, including privacy risk assessment, privacy impact assessment, privacy compliance review and other processes, and conduct regular compliance self-examination and revision. Security audit and vulnerability fixing: Conduct regular security audits to discover and fix possible security vulnerabilities and weaknesses in the system to ensure the security and privacy protection level of the system. TPOS risk management: For data processing involving TPOS service providers, establish appropriate contractual and regulatory mechanisms to ensure TPOS compliance and appropriate privacy protection measures.

When designing and implementing a privacy protection plan, it is necessary to comprehensively consider technical, organizational, legal, and personnel factors to ensure the effectiveness and comprehensiveness of privacy protection measures. At the same time, it is necessary to pay close attention to the latest developments and technological progress in the field of privacy protection, and update and strengthen the privacy protection plan in a timely manner.

5. Conclusions

Car owner information privacy protection is an important means to protect the rights and interests of car owners and maintain social harmony and stability. In the Internet of Vehicles, there is a large amount of privacy data involving the location, running trajectory, home address, work unit, personal information, line signals, and surrounding environment information of the user's vehicle. Once leaked, it may lead to serious consequences and even threaten national security.

Choose and share carefully: Carefully choose the platforms and service providers with which you share your personal information. Before providing personal information, you should understand its privacy policy and information protection measures, and choose reliable platforms and service providers. Control disclosure of information: Provide personal information only when necessary and disclose it only to trusted institutions or individuals. Avoid leaking personal information to unknown sources or suspicious third parties.

Strengthen password and account security: Set strong passwords and change them regularly, and use security mechanisms such as two-factor authentication to protect the security of personal accounts. Avoid logging into personal accounts in public places or unsafe network environments. Regularly check and update privacy settings: Regularly check and update privacy settings on mobile phones, car systems, and other devices to ensure that personal information is protected. Even if the attacker can obtain the pseudonym of one of the vehicles, he cannot tell which vehicle the pseudonym belongs to, further protecting the location privacy of the vehicle.

Beware of scams: Stay vigilant and avoid clicking on suspicious links or downloading unverified apps to prevent the theft and misuse of personal information. Strengthen data backup and back up important data regularly to prevent data loss or ransomware attacks. Car owners should enhance their awareness of privacy protection, understand relevant laws and regulations, and actively take measures to protect the security of personal information.

References

[1] Chen Yanhua, Li Jiangyin, An Qiyu. Analysis of personal privacy compliance of smart terminal mobile application App in the era of big data[J]. Quality and Certification, 2023,(11):63-66.DOI: 10.16691/j.cnki.10-1214/t.2023.11.006

ISSN 2706-655X Vol.5, Issue 12: 111-117, DOI: 10.25236/IJFET.2023.051217

[2] Shen Zihao, Gao Yongsheng, Wang Hui, et al. Deep Deterministic Policy Gradient Caching Method for Privacy Protection of Internet of Vehicles[J/OL]. Journal of Jilin University (Engineering Science),1-9[2023-12-06] https://doi.org/10.13229/j.cnki.jdxbgxb.20230908
[3] Sun Kai, Bai Zhezhe, Han Zhijun. Research on data security protection technology for Internet of Vehicles [J]. Information Security and Communication Confidentiality, 2023,(07):63-69
[4] Liu Qi, Zhang Jie. Research on location privacy protection scheme for Internet of Vehicles[J]. Information Technology and Informatization, 2023, (04):79-82